DIALOG(R)File 35 erwent WPI

012615735 **Image available**
WPI Acc No: 1999-421839/ 199936
XRPX Acc No: N99-315239
Authentication of digital images
Patent Assignee: THOMSON MULTIMEDIA (THOH); THOMSON MULTIMEDIA SA (THOH)
Inventor: BOYER R; CHEVREAU S; MEUNIER P; STARON A; MEUNIER P L
Number of Countries: 020 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2772530	A1	19990618	FR 9716008	A	19971217	199936	B
WO 9931844	A1	19990624	WO 98FR2730	A	19981215	199936	
EP 1040619	A1	20001004	EP 98959987	A	19981215	200050	
			WO 98FR2730	A	19981215		

Priority Applications (No Type Date): FR 9716008 A 19971217
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2772530	A1		18	H04L-009/00	
WO 9931844	A1	F		H04L-009/32	
Designated States (National): JP US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1040619	A1	F		H04L-009/32	Based on patent WO 9931844
Designated States (Regional): DE FR GB					

Abstract (Basic): **FR 2772530** A1

NOVELTY - The system uses public key cryptography and segments camera output and attaches a digital signature to successive parts (F1(VN)) of the image. The signature uses the secret key (K1). The camera output is constructed by multiplexing the raw signal with the segments and their signature. The validation device demultiplexes camera output and uses the public key (K2) to validate the image.

USE - Digital images from camera

ADVANTAGE - Provides proof that an image has not been falsified, providing publishing media with confidence in dealing with varied information sources, including freelance journalists.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of the system

) Fragment of image (F1(VN)

Secret key (K1)

Public key (K2)

pp; 18 DwgNo 1/3

Title Terms: AUTHENTICITY; DIGITAL; IMAGE
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00; H04L-009/32
International Patent Class (Additional): G06T-009/00
File Segment: EPI

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** 2 772 530
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** 97 16008

(51) Int Cl[6] : **H 04 L 9/00**, G 06 T 9/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.12.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.06.99 Bulletin 99/24.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *THOMSON MULTIMEDIA Societe anonyme* — FR.

(72) **Inventeur(s) :** CHEVREAU SYLVAIN, MEUNIER PAUL LOUIS, BOYER ROBERT et STARON ALAIN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** THOMSON MULTIMEDIA.

(54) PROCEDE D'AUTHENTIFICATION D'IMAGES NUMERIQUES ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE.

(57) L'invention concerne un procédé d'authentification d'images numériques ainsi qu'un système mettant en oeuvre le procédé.

Le système mettant en oeuvre le procédé comprend un dispositif de prise de vues -caméra ou appareil photo- etun dispositif de traitement des informations issues du dispositif de prise de vues.

Le dispositif de prise de vues comprend des moyens pour hacher et signer des fractions successives du signal filmé ou photographié. Le signal issu du dispositif de prise de vues est construit par multiplexage du signal en clair et des fractions de signal hachées et signées.

Le dispositif de traitement comprend un démultiplexeur pour séparer les données hachées et signées du signal en clair, des moyens pour hacher les fractions de signal qui correspondent aux fractions de signal qui ont été hachées et signées dans le dispositif de prise de vues, des moyens pour effectuer un chiffrement à clé publique des fractions de signal hachées et signées, et des moyens pour comparer les fractions de signal hachées dans le dispositif de traitement aux données issues de l'opération de chiffrement à clé publique.

Le signal issu du comparateur permet alors d'indiquer si les images numériques qui ont été filmées sont authentiques ou falsifiées.

L'invention s'applique plus particulièrement aux caméras de reportage du domaine professionnel.

FR 2 772 530 - A1

PROCEDE D'AUTHENTIFICATION D'IMAGES NUMERIQUES ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE

La présente invention concerne un procédé d'authentification de données numériques et un dispositif mettant en oeuvre le procédé.

L'invention s'applique plus particulièrement à l'authentification d'images numériques issues d'un appareil de prise de vues tel que, par exemple, une tête de caméra ou un appareil photographique.

Les images numériques sont des images falsifiables. Ainsi en est-il, par exemple, des images numériques constituant un reportage d'actualités ou une émission de télévision, que ces images soient diffusées en direct ou à partir d'une source de données enregistrées.

Les personnes à qui sont transmises des images numériques se trouvent donc dans une situation où l'authenticité des informations qu'elles reçoivent n'est pas garantie. Cet inconvénient est d'autant plus important que se multiplient les sources d'informations telles que, par exemple, les sources d'informations provenant de journalistes communément appelés journalistes "free-lances".

L'invention ne présente pas cet inconvénient.

En effet, la présente invention concerne un procédé d'authentification d'images constituées de données numériques. Le procédé comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction des données numériques,
- une étape de hachage de la première fraction prélevée afin de générer une première donnée hachée,
- une étape de déchiffrement à clé secrète K1 de la première donnée hachée de façon à constituer une signature de la première donnée hachée,
- une étape de multiplexage des données numériques et de la signature,
- une étape de démultiplexage des données numériques et de la signature,
- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'au moins une deuxième fraction des données numériques, la deuxième fraction contenant des données de même type que les données contenues dans la première fraction,

- une étape de chiffrement à clé publique K2 de la signature de façon à constituer une donnée chiffrée, la clé publique K2 étant couplée à la clé secrète K1 selon le principe de la cryptographie à clé publique,

- une étape de hachage de la deuxième fraction de façon à constituer une deuxième donnée hachée,

- une étape de comparaison de la deuxième donnée hachée et de la donnée chiffrée permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

L'invention concerne également un procédé de signature d'images constituées de données numériques. Le procédé comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction des données numériques,

- une étape de hachage de la première fraction prélevée afin de générer une première donnée hachée,

- une étape de déchiffrement à clé secrète K1 de la première donnée hachée de façon à constituer une signature de la première donnée hachée,

- une étape de multiplexage des données numériques et de la signature de façon à constituer un signal multiplexé.

L'invention concerne également un procédé d'authentification d'images numériques issues d'un procédé de signature tel que celui selon l'invention mentionné ci-dessus. Le procédé comprend :

- une étape de démultiplexage du signal multiplexé de façon à séparer les données numériques et la signature,

- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'une deuxième fraction des données numériques, la deuxième fraction contenant des données de même type que les données contenues dans la première fraction,

- une étape de chiffrement à clé publique K2 de la signature de façon à constituer une donnée chiffrée, la clé publique K2 étant couplée, selon le principe de la cryptographie à clé publique, à la clé secrète K1 du procédé de signature,

- une étape de hachage de la deuxième fraction de façon à constituer une deuxième donnée hachée,

- une étape de comparaison de la deuxième donnée hachée et de la donnée chiffrée permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

L'invention concerne également un premier sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques. Le premier sous-ensemble comprend un appareil de prise de vues et un élément de sécurité, l'appareil de prise de vues comprenant un circuit d'interface avec l'élément de sécurité, un circuit de multiplexage et un circuit de hachage d'au moins une première fraction des données numériques de façon à générer une première donnée hachée, l'élément de sécurité comprenant un circuit de déchiffrement à clé secrète K1 de la première donnée hachée de façon à générer une signature de la première donnée hachée, la signature et les données numériques étant transmises au circuit de multiplexage de façon à constituer un signal multiplexé.

L'invention concerne également un second sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques. Le second sous-ensemble comprend un appareil de prise de vues et un élément de sécurité, l'appareil de prise de vues comprenant un circuit d'interface avec l'élément de sécurité et un circuit de multiplexage, l'élément de sécurité comprenant un circuit de hachage d'au moins une première fraction des données numériques provenant de l'appareil de prise de vues de façon à générer une première donnée hachée et un circuit de déchiffrement à clé secrète K1 de la première donnée hachée de façon à générer une signature de la première donnée hachée, la signature issue de l'élément de sécurité et les données numériques étant transmises au circuit de multiplexage de façon à constituer un signal multiplexé.

L'invention concerne encore un appareil de prise de vues permettant de transformer un signal lumineux représentant au moins une image en un signal constitué de données numériques. L'appareil comprend des moyens permettant d'authentifier les données numériques.

L'invention concerne encore un sous-ensemble permettant l'authentification de données numériques issues d'un sous-ensemble permettant d'authentifier la prise de vues d'images tel que le premier ou le second sous-ensemble selon l'invention mentionné ci-dessus ou d'un appareil tel que l'appareil selon l'invention mentionné ci-dessus. Le sous-ensemble comprend un démultiplexeur permettant de séparer les données vidéo numériques et la signature, un circuit de chiffrement à clé publique K2 permettant de calculer une donnée chiffrée à partir de la signature, un circuit de hachage d'au moins une deuxième fraction des données vidéo numériques issues du démultiplexeur de façon à générer une deuxième donnée hachée, un circuit de comparaison permettant de comparer la donnée chiffrée avec la deuxième donnée hachée de façon à constituer un signal permettant de vérifier l'authenticité des données numériques.

L'invention concerne encore une unité de contrôle permettant de traiter le signal numérique issu d'une tête de caméra. L'unité de contrôle comprend un sous-ensemble permettant l'authentification de données numériques tel que celui selon l'invention mentionné ci-dessus.

L'invention concerne encore un système permettant l'authentification d'images constituées de données numériques. Le système comprend un sous-ensemble permettant d'authentifier la prise de vues d'images tel que le premier ou le second sous-ensemble selon l'invention mentionné ci-dessus ou un appareil tel que l'appareil selon l'invention mentionné ci-dessus et un sous-ensemble permettant l'authentification de données numériques tel que celui selon l'invention mentionné ci-dessus.

Un avantage de l'invention est d'authentifier les images numériques issues d'un dispositif de prise de vues. L'invention s'applique avantageusement aussi bien au cas où les images à authentifier sont des images prises en direct qu'au cas où les images à authentifier sont des images issues d'une source enregistrée.

D'autres avantages et caractéristiques de l'invention apparaîtront à la lecture d'un mode de réalisation préférentiel fait en référence aux figures ci-annexées parmi lesquelles :

- la figure 1 représente un premier dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention ;

- la figure 2 représente un deuxième dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention ;

- la figure 3 représente, selon l'invention, un dispositif d'authentification d'images numériques issues d'un dispositif de prise de vues tel que celui représenté en figure 1 ou en figure 2.

Sur toutes les figures, les mêmes repères désignent les mêmes éléments.

La figure 1 représente un premier dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention.

Le dispositif de prise de vues est constitué d'un appareil de prise de vues 1 et d'un élément de sécurité 2. L'appareil de prise de vues 1 peut être, par exemple, une tête de caméra ou un appareil photographique. Selon le mode de réalisation préférentiel de l'invention, l'élément de sécurité est un élément détachable tel que, par exemple, une carte à puce.

L'appareil de prise de vues 1 comprend un objectif 3, un bloc 4 de circuits de traitement du signal issu de l'objectif 3, un circuit de hachage 5, un multiplexeur 6 et un circuit 7 d'interface avec la carte à puce.

De façon connue en soi, l'objectif 3 et le bloc 4 de circuits de traitement permettent de transformer un signal lumineux L en un signal numérique VN.

Selon l'invention, une fraction F1(VN) du signal numérique VN est prélevée, préférentiellement de façon régulière, en sortie du bloc 4. Chaque fraction F1(VN) prélevée est transmise au circuit de hachage 5. Le circuit 5 peut être un circuit électronique ou un élément logiciel. A titre d'exemples non limitatifs, la fraction F1(VN) du signal numérique VN peut être composée des lignes paires ou impaires d'une même image ou des données relatives à la composante de luminance d'une même image. La fraction F1(VN) peut également être constituée de plusieurs trames prélevées à intervalles de temps réguliers dans le cas d'une tête de caméra ou image par image dans le cas d'un appareil photo. De façon générale, la donnée F1(VN) est composée de données significatives d'une image.

Le résultat m1 issu de la fonction de hachage du signal F1(VN) est transmis au circuit d'interface 7. La donnée m1 comprend, par exemple, quelques dizaines de bits.

Le circuit d'interface 7 permet le transfert bidirectionnel de données entre l'appareil 1 et la carte à puce 2. De façon préférentielle, le circuit 7 est un circuit d'interface série bidirectionnel au standard ISO-7816.

La carte à puce contient un circuit de déchiffrement (non représenté sur la figure) ainsi qu'une clé secrète K1. De façon préférentielle, la clé K1 est stockée dans une mémoire programmable contenue dans la carte 2. Sous l'action de la clé K1, les données m1 successives transmises à la carte 2 sont déchiffrées par le circuit de déchiffrement de façon à constituer une suite de données $D(m1)_{K1}$. Chaque donnée $D(m1)_{K1}$ constitue la signature de la donnée m1 et donc de la fraction F1(VN) d'où est issue la donnée m1.

Par l'intermédiaire du circuit d'interface 7, les données $D(m1)_{K1}$ sont transmises de la carte à puce 2 vers une première entrée du multiplexeur 6 qui reçoit, par ailleurs, le signal numérique VN sur une deuxième de ses entrées.

Le signal S1 issu du multiplexeur 6 est alors composé des données numériques VN et des données $D(m1)_{K1}$. De façon préférentielle, chaque donnée $D(m1)_{K1}$ est insérée dans un en-tête associé à la fraction de donnée F1(VN) qui lui correspond. Selon un autre mode de réalisation de l'invention, les données $D(m1)_{K1}$ sont substituées à certaines des données VN qui sont alors perdues.

La figure 2 représente un deuxième dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention.

Le dispositif de prise de vues est constitué d'un appareil de prise de vues 8 et d'un élément de sécurité 9. L'élément de sécurité est un élément détachable tel que, par exemple, une carte à puce. L'appareil 8 peut être, par exemple, une tête de caméra ou un appareil photographique. L'appareil 8 contient les mêmes circuits que l'appareil 1 décrit à la figure 1 à l'exception du circuit de hachage 5.

Selon le mode de réalisation de la figure 2, la fonction de hachage est réalisée dans la carte à puce 9. Il s'ensuit que la fraction F1(VN) du signal numérique VN est transmise à la carte à puce 9.

De même que mentionné ci-dessus, le hachage de la donnée F1(VN) génère une donnée m1 qui, déchiffrée, génère une donnée $D(m1)_{K1}$. Par l'intermédiaire du circuit d'interface 7 les données successives $D(m1)_{K1}$ sont transmises de la carte à puce 9 vers le multiplexeur 6. Le signal S1 issu de l'appareil de prise de vues 8 est alors généré comme mentionné précédemment.

Selon le mode de réalisation préférentiel de l'invention décrit aux figures 1 et 2, l'élément de sécurité est un élément détachable. L'invention concerne cependant un autre mode de réalisation pour lequel l'élément de sécurité n'est pas détachable. Le circuit de déchiffrement à clé secrète K1 et le circuit de hachage 5 sont alors tous deux intégrés dans l'appareil de prise de vues lui-même.

Un dispositif de prise de vues selon l'invention, que l'élément de sécurité soit ou non détachable, peut fonctionner, toutes choses égales par ailleurs, avec des clés de déchiffrement K1 ayant des valeurs différentes. Une même clé K1 peut alors être propre à une seule personne ou à un ensemble de personnes constituant, par exemple, un groupement de journalistes. Il s'ensuit qu'un avantage supplémentaire de l'invention est de garantir la provenance des images authentifiées.

L'utilisation d'un élément de sécurité détachable et protégé, tel que, par exemple, une carte à puce, est un avantage du mode de réalisation préférentiel de l'invention. D'une part, la carte à puce assure une fonction de clé personnelle dont la clé est secrète. D'autre part, l'utilisation d'une carte à puce implique que soit mis en oeuvre un processus d'identification mutuelle entre la carte à puce et le dispositif récepteur de la carte à puce, à savoir l'appareil de prise de vues. Il s'ensuit que le niveau de sécurité relatif aux différentes étapes mises en oeuvre dans la carte à puce et le dispositif de prise de vues est un niveau de sécurité élevé.

La figure 3 représente, selon l'invention, un dispositif d'authentification d'images numériques issues d'un dispositif de prise de vues tel que celui représenté en figure 1 ou en figure 2, que l'élément de sécurité soit ou non détachable.

Le dispositif 10 d'authentification d'images numériques comprend un démultiplexeur 11, un circuit 12 de chiffrement à clé publique K2, un circuit 13 de

hachage et un comparateur 14. Le démultiplexeur 11 reçoit sur son entrée un signal S1 tel que celui mentionné aux figures 1 et 2. Le signal S1 provient soit d'un dispositif de prise de vues tel que celui décrit aux figures 1 et 2, soit d'une source de données enregistrées telle que, par exemple, une bande magnétique, un disque vidéo numérique ou encore une disquette.

Le démultiplexeur 11 a pour fonction de séparer les données $D(m1)_{K1}$ des données numériques VN. Les données $D(m1)_{K1}$ sont transmises au circuit 12 de chiffrement à clé publique K2.

L'opération de chiffrement à clé publique K2 d'une donnée $D(m1)_{K1}$ conduit à calculer une donnée chiffrée $C(D(m1)_{K1})_{K2}$.

Selon l'invention, des fractions F2(VN) du signal numérique VN sont prélevées en sortie du démultiplexeur 11. Le prélèvement des fractions F2(VN) s'effectue à l'image du prélèvement des fractions F1(VN). Ainsi, chaque fraction F2(VN) correspond-elle à une fraction F1(VN) et les données qui sont contenues dans la fraction F2(VN) qui correspond à la fraction F1(VN) sont des données de même type que les données contenues dans la fraction F1(VN). Par "données de même type", il faut entendre que les données qui constituent la fraction F2(VN) sont des données a priori identiques aux données qui constituent la fraction F1(VN) qui lui correspond : les données sont identiques si la fraction F1(VN) n'a pas été falsifiée et différentes, en tout ou partie, si la fraction F1(VN) a été falsifiée.

Dans tous les cas, les données contenues dans une fraction F2(VN) représentent le même signal que les données contenues dans la fraction F1(VN) qui lui correspond. Ainsi, par exemple, si les données contenues dans une fraction F1(VN) sont constituées des lignes paires d'une image, les données contenues dans la fraction F2(VN) qui correspond à la fraction F1(VN) sont-elles constituées des lignes paires de la même image.

Le circuit 13 opère le hachage des données contenues dans les fractions F2(VN). L'opération de hachage effectuée par le circuit 13 est identique à celle effectuée par le circuit 5. Il s'ensuit que la donnée m2 qui est associée à une fraction F2(VN) correspondant à une fraction F1(VN) est identique à la donnée m1 qui est associée à la fraction F1(VN) si la fraction F1(VN) n'a pas été falsifiée. La donnée m2 issue du circuit 13 et la donnée $C(D(m1)_{K1})_{K2}$ sont transmises au comparateur 14.

Le signal S3 issu du comparateur 14 permet alors d'indiquer si les données numériques VN sont des données authentiques ou des données falsifiées : ce sont des données pouvant être considérées comme authentiques si chaque donnée m2 est égale à la donnée $C(D(m1)_{K1})_{K2}$ qui lui correspond, ce sont des données dont on sait qu'elles ont été falsifiées si au moins une donnée m2 est différente de la donnée $C(D(m1)_{K1})_{K2}$ qui lui correspond.

Selon l'invention, le dispositif 10 d'authentification d'images peut être intégré dans une unité de contrôle recevant des images filmées par une tête de caméra.

REVENDICATIONS

1. Procédé d'authentification d'images constituées de données numériques, caractérisé en ce qu'il comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction (F1(VN)) des données numériques (VN),
- une étape de hachage (5) de la première fraction prélevée (F1(VN)) afin de générer une première donnée hachée (m1),
- une étape de déchiffrement à clé secrète K1 de la première donnée hachée (m1) de façon à constituer une signature $(D(m1)_{K1})$ de la première donnée hachée (m1),
- une étape de multiplexage des données numériques (VN) et de la signature $(D(m1)_{K1})$,
- une étape de démultiplexage (11) des données numériques (VN) et de la signature $(D(m1)_{K1})$,
- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'au moins une deuxième fraction (F2(VN)) des données numériques, la deuxième fraction (F2(VN)) contenant des données de même type que les données contenues dans la première fraction (F1(VN)),
- une étape de chiffrement à clé publique K2 de la signature $(D(m1)_{K1})$ de façon à constituer une donnée chiffrée $(C\ (D(m1)_{K1})_{K2})$, la clé publique K2 étant couplée à la clé secrète K1 selon le principe de la cryptographie à clé publique,
- une étape de hachage (13) de la deuxième fraction (F2(VN)) de façon à constituer une deuxième donnée hachée (m2),
- une étape de comparaison (14) de la deuxième donnée hachée (m2) et de la donnée chiffrée $(C(D(m1)_{K1})_{K2})$ permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

2. Procédé de signature d'images constituées de données numériques, caractérisé en ce qu'il comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction (F1(VN)) des données numériques (VN),
- une étape de hachage (5) de la première fraction prélevée (F1(VN)) afin de générer une première donnée hachée (m1),

- une étape de déchiffrement à clé secrète K1 de la première donnée hachée (m1) de façon à constituer une signature ($D(m1)_{K1}$) de la première donnée hachée (m1),

- une étape de multiplexage des données numériques (VN) et de la signature ($D(m1)_{K1}$) de façon à constituer un signal multiplexé (S1).

3. Procédé d'authentification d'images numériques issues d'un procédé de signature selon la revendication 2, caractérisé en ce qu'il comprend :

- une étape de démultiplexage (11) du signal multiplexé (S1) de façon à séparer les données numériques (VN) et la signature ($D(m1)_{K1}$),

- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'une deuxième fraction (F2(VN)) des données numériques, la deuxième fraction (F2(VN)) contenant des données de même type que les données contenues dans la première fraction (F1(VN)),

- une étape de chiffrement à clé publique K2 de la signature ($D(m1)_{K1}$) de façon à constituer une donnée chiffrée ($C\ (D(m1)_{K1})_{K2}$), la clé publique K2 étant couplée, selon le principe de la cryptographie à clé publique, à la clé secrète K1 du procédé de signature,

- une étape de hachage (13) de la deuxième fraction (F2(VN)) de façon à constituer une deuxième donnée hachée (m2),

- une étape de comparaison (14) de la deuxième donnée hachée (m2) et de la donnée chiffrée ($C(D(m1)_{K1})_{K2}$) permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

4. Sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques (VN), caractérisé en ce qu'il comprend un appareil (1) de prise de vues et un élément de sécurité (2), l'appareil (1) de prise de vues comprenant un circuit d'interface (7) avec l'élément de sécurité, un circuit de multiplexage (6) et un circuit de hachage (5) d'au moins une première fraction (F1(VN)) des données numériques de façon à générer une première donnée hachée (m1), l'élément de sécurité (2) comprenant un circuit de déchiffrement à clé secrète K1 de la première donnée hachée (m1) de façon à générer une signature ($D(m1)_{K1}$) de la première donnée hachée (m1), la signature ($D(m1)_{K1}$) et les données

numériques (VN) étant transmises au circuit de multiplexage (6) de façon à constituer un signal multiplexé (S1).

5. Sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques (VN), caractérisé en ce qu'il comprend un appareil (8) de prise de vues et un élément de sécurité (9), l'appareil (8) de prise de vues comprenant un circuit d'interface (7) avec l'élément de sécurité et un circuit de multiplexage (6), l'élément de sécurité (2) comprenant un circuit de hachage d'au moins une première fraction (F1(VN)) des données numériques provenant de l'appareil de prise de vues (8) de façon à générer une première donnée hachée (m1) et un circuit de déchiffrement à clé secrète K1 de la première donnée hachée (m1) de façon à générer une signature $(D(m1)_{K1})$ de la première donnée hachée (m1), la signature $(D(m1)_{K1})$ issue de l'élément de sécurité et les données numériques (VN) étant transmises au circuit de multiplexage (6) de façon à constituer un signal multiplexé (S1).

6. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que l'appareil (1, 8) de prise de vues est une tête de caméra.

7. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que l'appareil (1, 8) de prise de vues est un appareil photographique.

8. Sous-ensemble selon l'une quelconque des revendications 4 à 7, caractérisé en ce que l'élément de sécurité est une carte à puce.

9. Appareil de prise de vues (1, 8) permettant de transformer un signal lumineux (L) représentant au moins une image en un signal constitué de données numériques (VN), caractérisé en ce qu'il comprend des moyens permettant d'authentifier les données numériques (VN), les moyens permettant d'authentifier les données numériques comprenant un circuit d'interface (7) avec un élément de sécurité et un multiplexeur (6).

10. Appareil de prise de vues (1, 8) selon la revendication 9, caractérisé en ce qu'il comprend un circuit de hachage (5).

11. Appareil de prise de vues (1, 8) permettant de transformer un signal lumineux (L) représentant au moins une image en un signal constitué de données numériques (VN), caractérisé en ce qu'il comprend des moyens permettant d'authentifier les données numériques (VN), les moyens permettant d'authentifier les données numériques(VN) comprenant un circuit de hachage (5), un circuit de déchiffrement à clé secrète K1 et un multiplexeur (6).

12. Sous-ensemble permettant l'authentification de données numériques issues d'un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou d'un appareil selon la revendication 11, caractérisé en ce qu'il comprend un démultiplexeur (11) permettant de séparer les données numériques (VN) et la signature $(D(m1)_{K1})$, un circuit de chiffrement à clé publique K2 permettant de calculer une donnée chiffrée $(C(D(m1)_{K1})_{K2})$ à partir de la signature $(D(m1)_{K1})$, un circuit de hachage (13) d'au moins une deuxième fraction (F2(VN)) des données numériques (VN) issues du démultiplexeur (11) de façon à générer une deuxième donnée hachée (m2), un circuit de comparaison (14) permettant de comparer la donnée chiffrée $(C(D(m1)_{K1})_{K2})$ avec la deuxième donnée hachée (m2) de façon à constituer un signal (S3) permettant de vérifier l'authenticité des données numériques.

13. Unité de contrôle permettant de traiter le signal numérique issu d'une tête de caméra, caractérisée en ce qu'elle comprend un sous-ensemble selon la revendication 12.

14. Système permettant l'authentification d'images constituées de données numériques, caractérisé en ce qu'il comprend un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou un appareil selon la revendication 11 et un sous-ensemble selon la revendication 12.

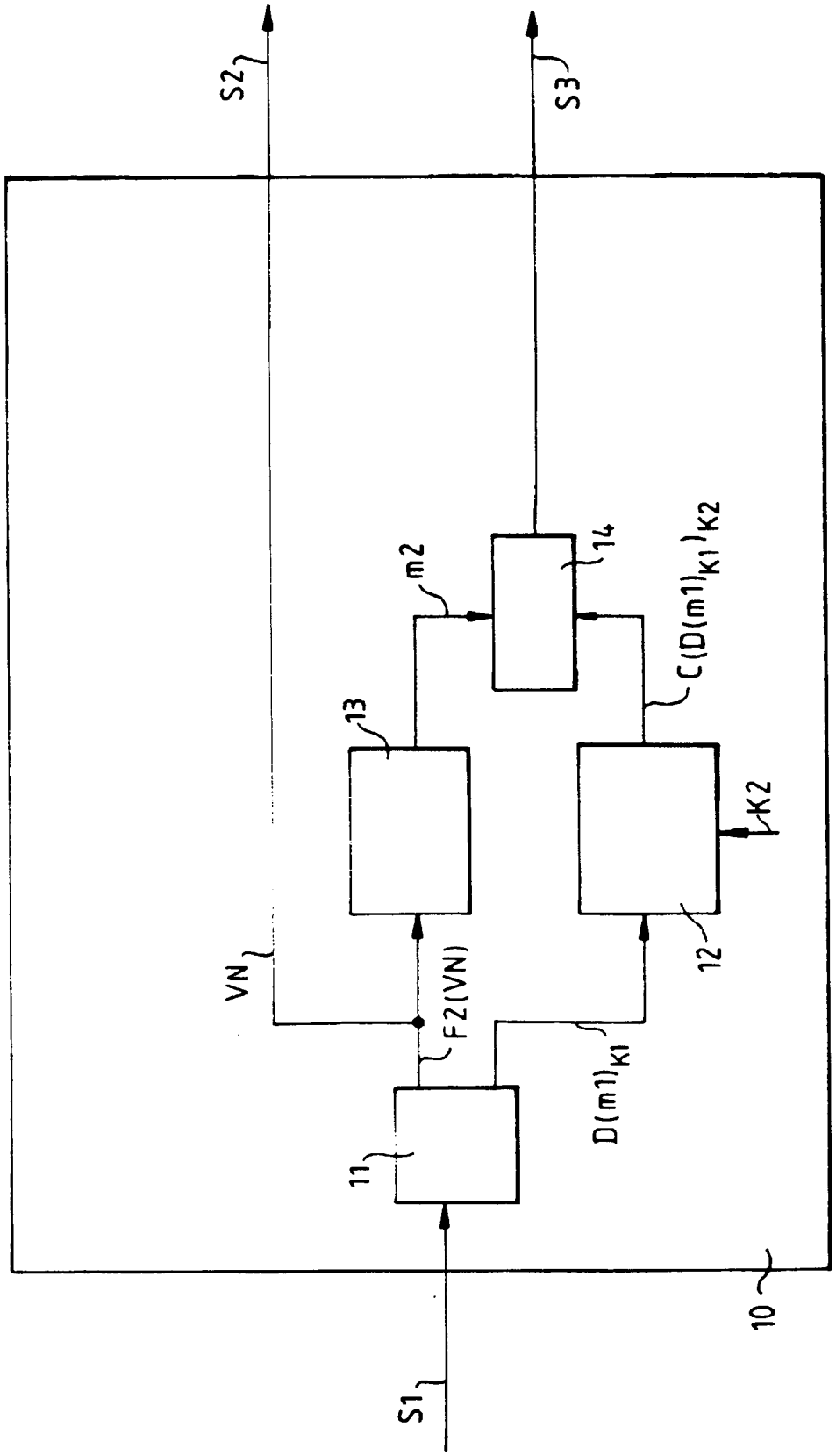

FIG.3

REPUBLIQUE FRANÇAISE

2772530

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 554991
FR 9716008

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US 5 499 294 A (FRIEDMAN GARY L) 12 mars 1996	1-3,9-11
A	* colonne 3, ligne 1 - ligne 6 * * colonne 7, ligne 6 - ligne 10 * * colonne 8, ligne 46 - colonne 9, ligne 6 * * colonne 5, ligne 49 - colonne 6, ligne 42 * * colonne 3, ligne 26 - ligne 34 * * colonne 4, ligne 26 - ligne 54 *	4-7, 12-14
A	EP 0 383 985 A (SCHNORR) 29 août 1990 * page 4, ligne 54 - page 5, ligne 21; revendication 3 *	8
A	EP 0 752 786 A (THOMSON CONSUMER ELECTRONICS) 8 janvier 1997 * page 2, ligne 28 - ligne 30 * * page 5, ligne 20 - ligne 29 * * page 6, ligne 29 - page 7, ligne 1; figure 7 *	1,2,4,9

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L

1

Date d'achèvement de la recherche	Examinateur
4 septembre 1998	Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

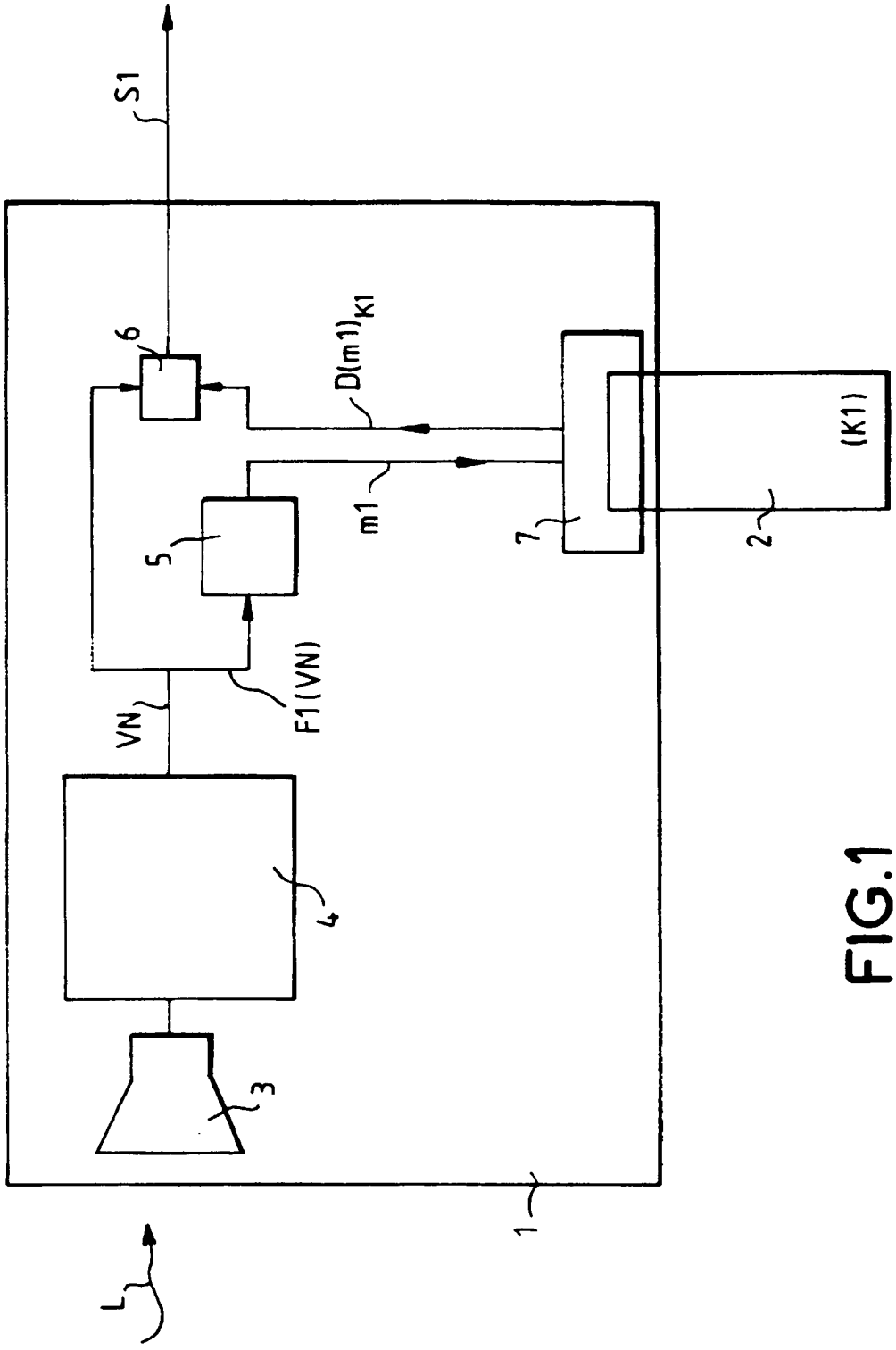

FIG.1

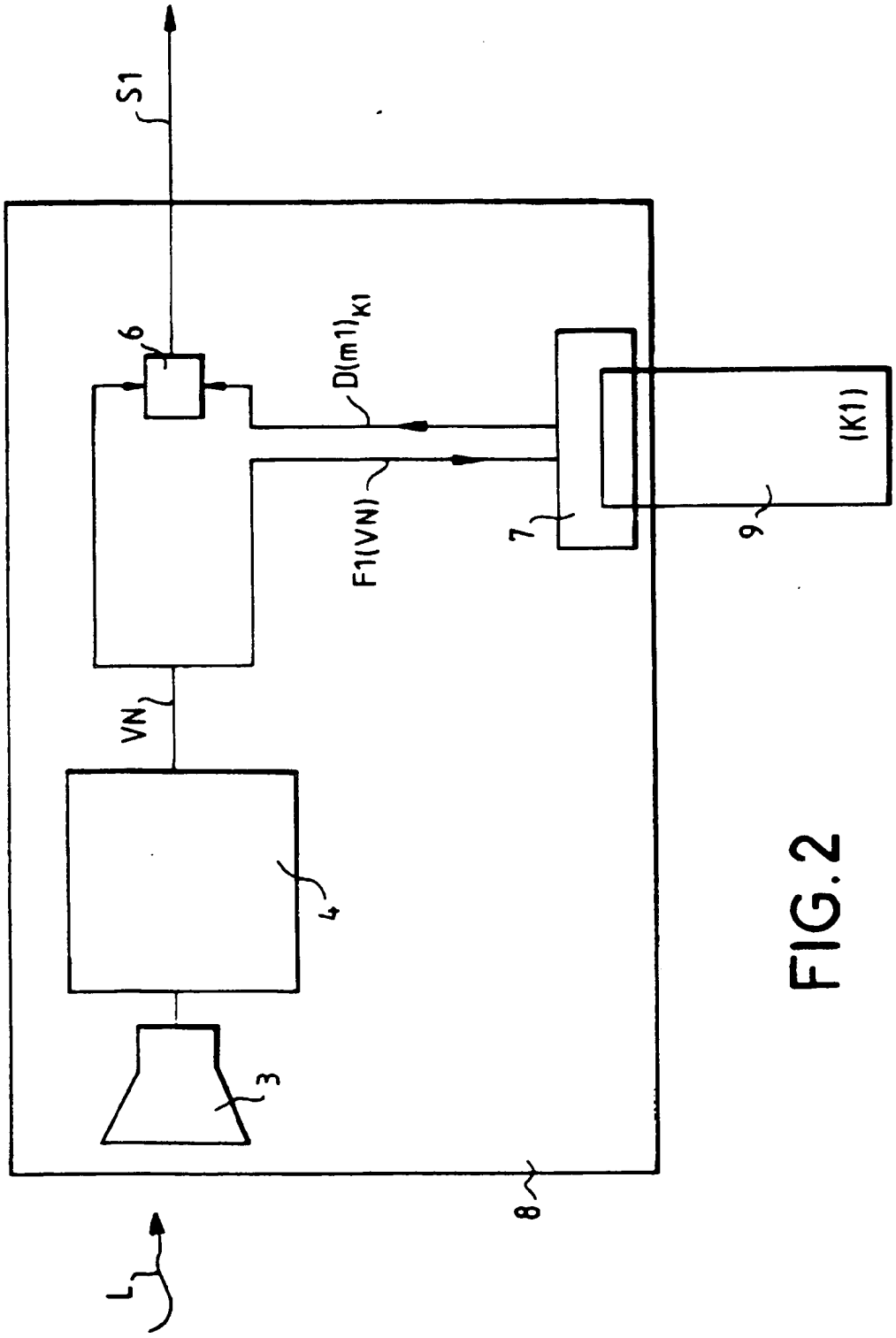

FIG.2